2. J. A. WARD, "The downhill method of solving $f(z) = 0$," *Jn.*, Assn. for Comp. Machinery., v. 4, 1957, p. 148.
3. L. CAGNIARD, *Réflexion et Réfraction des Ondes Seismiques Progressives*, Gauthier-Villars, Paris, 1939, p. 55–58.
4. A. S. HOUSEHOLDER, *Principles of Numerical Analysis*, McGraw-Hill, New York, 1953, p. 118–121.

A Problem in Abelian Groups, with Application to the Transposition of a Matrix on an Electronic Computer

By Gordon Pall and Esther Seiden

1. Introduction. Mr. G. A. Westlund of "Mura" (Midwestern Universities Research Association) was asked to formulate a code to transpose a matrix stored in the memory of IBM 704, using very little additional space. It appeared that such a code, by Mr. William Shooman of General Electric in Evendale, was already available and had been distributed on June 15, 1957, to SHARE members of IBM 704. Mr. Westlund asked whether there exists a more efficient method for this purpose.

A matrix of m rows and n columns is stored in the computer with the elements of each column listed in order and followed by those of the next column. The positions can be numbered as $mj + i$ $(i = 0, 1, \cdots, m - 1; j = 0, 1, \cdots, n - 1)$. To transpose the matrix, the element in position $mj + i$ must be moved to position $ni + j$. The key remark is that the new position number is obtained from the old by multiplication by n, and reducing mod $N(= mn - 1)$. Starting with any element (which we will call a *leader*), we multiply its position number by n and replace mod N, repeat this operation with the new position number again and again, and thus have a cycle of elements which are permuted cyclically in the process of transposing a matrix. If v is the g.c.d. of any of the position numbers and N, then the number of elements in the cycle is equal to the least positive integer r for which $n^r \equiv 1 (\mathrm{mod}\, N/v)$.

The questions then arise: (a) can a method be devised of choosing one and only one leader in every cycle; and (b) if this is done, will the new method of transposing a matrix compare favorably in machine time with the existing method? Both questions are answered affirmatively in this note.

A program for transposing a matrix, once a set of leaders is given, was constructed at our request by G. A. Westlund, under the direction of M. R. Storm, head of the computing section at Mura. The suggestion was made that our method for forming a set of leaders (see §2) might also be programmed by building a table of indices and primitive roots into the computer. We felt that it would be more economical to carry out the construction of a set of leaders by hand. The construction of a table of leaders for all pairs m, n with certain properties is under investigation.

In transposing a matrix by the Mura program, the machine time is much smaller

Received August 4, 1958; revised September 8, 1959.

than that by the General Electric method (Matrix Transposed on Itself, Shooman at Evendale, June 21, 1957). By the latter method the total number of switches is $m(m-1)n(n-1)/4$, and is roughly proportional to the square of the number of elements of the matrix. By our method the number of switches is roughly proportional to the number of elements of the matrix. Here are some examples of machine times.

Size of matrix.	Time by Mura Program.	Time by G. E. program.
8 by 7	Too small to measure	Too small to measure
21 by 14	Too small to measure	2.5 seconds
18 by 15	Too small to measure	2 seconds
31 by 8	Too small to measure	2 seconds
24 by 35	Less than a second	23 seconds
23 by 25	Less than a second	20.5 seconds
25 by 31	Less than a second	21 seconds
75 by 73	Less than five seconds	17.5 minutes.

2. Background Theory. Let G be the group of residues prime to N modulo N, and let n be an integer prime to N. We will give an algorithm for choosing a set $S(n, N)$, containing exactly one element of each coset in G of the group of powers of n modulo N.

It seems necessary to remark that it seems not to be trivial—as we at first supposed—to devise a *general* method of choosing a complete set of representatives of a group modulo a subgroup—if one does not wish to take the time to write out coset after coset, and *see* what remains. Notice for example that if p and q are distinct primes, and if p divides $q-1$, the solvability for x of $an^x \equiv b \pmod{p^r}$ and for y of $an^y \equiv b \pmod{q^s}$ may impose on x and y inconsistent conditions modulo p,—and so a and b can be in the same coset mod p^r and mod q^s without being so for their product. It will be seen in the vector representation which follows that now one and now another of the components dominates the congruence conditions, and an unsystematic analysis may be difficult. Perhaps indeed our algorithm may have value beyond this present application.

As is well known, if $p = p_i$ is an odd prime, and $t = t_i$ a positive integer, there is an integer $g = g_i$ (a primitive root of p^t) such that every residue k prime to p modulo p^t is associated uniquely with an index e mod N_i, where

$$N_i = p_i^{t_i-1}(p_i - 1), \tag{1}$$

such that $k \equiv g^e \pmod{p^t}$. If $p = 2$ and $t \geqq 2$, there are two indices e_0 and e_1 corresponding to any given odd residue k mod 2^t such that

$$k \equiv (-1)^{e_0}5^{e_1} \pmod{2^t}, \quad \text{with } e_0 \text{ determined mod } N_0, \quad \text{and } e_1 \text{ mod } N_1, \tag{2}$$

where $N_0 = 2$ and $N_1 = 2^{t-2}$. This extends to $t = 1$ if we choose $N_0 = N_1 = 1$. Index tables exist for prime-powers up to 10,000 from which corresponding values k and e, or k and e_0, e_1 may be read.

Write $N = p_1^{t_1} \cdots p_s^{t_s}$ as a product of powers of distinct primes. If N is even, take $p_1 = 2$ and N_0, N_1 as above; otherwise use (1). Then by the preceding paragraph and the Chinese Remainder Theorem, there is associated with each residue prime to N modulo N a unique index vector $(e_h, e_{h+1}, \cdots, e_s)$ with components

determined respectively to the moduli $N_h, \cdots, N_s$; h is 0 or 1 according as N is even or odd. The group G is isomorphic to the "additive group" of these vectors.

3. The Algorithm. Find the index vector $(u_h, \cdots, u_s)$ of n. Find the g.c.d. d_i of N_i and u_i, and set $K_i = N_i/d_i$, $i = h, \cdots, s$. For each prime p dividing $K_h \cdots K_s$, let $j(=j_p)$ denote the subscript of that one (or of any *one*) of $K_h, \cdots, K_s$ which contains the highest power of p. (We will speak of p as *belonging to* j.) For each i from h to s, write $K_i = L_iQ_i$, where Q_i consists of the prime factors belonging to i. (Thus L_i is prime to Q_i, and Q_i may be 1.) Let S_i denote the set of L_i residues mod K_i obtained by combining each of 0, 1, $\cdots$, $L_i - 1$ with any desired fixed residue mod Q_i. (For example, S_i can be)

$$k, k + Q_i, k + 2Q_i, \cdots, k + (L_i - 1)Q_i, \quad k \text{ a fixed integer.})$$

Then, a set $S(n, N)$ is given by the vectors

$$(3) \quad (e_h + d_hy_h, \cdots, e_s + d_sy_s), \qquad \textit{with } y_i \textit{ ranging over } S_i,$$
$$\textit{and } e_i = 0, 1, \cdots, d_i - 1, \quad (i = h, \cdots, s).$$

Proof. Notice first that the order of the cyclic group generated by n is equal to the least positive integer q such that

$$(4) \qquad qu_i \equiv 0 \pmod{N_i}, \qquad (i = h, \cdots, s),$$

and that $q = Q_h \cdots Q_s$. Also, the number of vectors in (3) is $d_h \cdots d_sL_h \cdots L_s = N_h \cdots N_s/q$. Hence we have only to prove that no two of these vectors are in the same coset. Notice also that the coset of any given vector $(z_h, \cdots, z_s)$ is composed of the q vectors

$$(z_h + xu_h, \cdots, z_s + xu_s), \qquad x = 0, 1, \cdots, q - 1;$$

and for each i, the components $z_i + xu_i$ have a fixed residue modulo d_i. Hence if two vectors in (3), say $(z_h, \cdots, z_s)$ and $(z_h + xu_h, \cdots, z_s + xu_s)$, are in the same coset, they must have the same terms $e_h, \cdots, e_s$ and, for each prime p and the subscript j to which p belongs, $z_j \equiv z_j + xu_j$ modulo the power of p in N_j (since, for every i, $z_i \equiv z_i + xu_i \bmod d_iQ_i$). Hence xu_j is divisible by the power of p in N_j. But (excluding the trivial case where all indices $u_h, \cdots, u_s$ are 0, hence $n = 1$) N_j and qu_j contain the same power of p. Hence xu_j is divisible by the power of p in qu_j, x by the power of p in q (this for every p), x is divisible by q, and the two vectors coincide. Q.E.D.

It remains to convert the vectors in (3) into position numbers mod N. Write $M_i = N/p_i^{t_i}$ $(i = 1, \cdots, s)$. The expression

$$(5) \qquad M_1g_1^{e_1+d_1y_1} + \cdots + M_sg_s^{e_s+d_sy_s},$$

the first term being replaced if N is even by $M_1(-1)^{e_0+d_0y_0}5^{e_1+d_1y_1}$, e_i and y_i having the ranges in (3), gives exactly one leader in every cycle whose position numbers are prime to N. (One can of course read off the values g^{e+dy} from the index table.) Because of the factors M_i the leaders listed in (5) may not be exactly those specified in (3), since the expression in (5) gives the number with g_i to the index $e_i' + e_i + d_i(y_i + y_i')$, where $e_i' + d_iy_i'$ is the index of M_i. But

since e_i' and y_i' are fixed for each i, this has the effect of permuting the residues $e_i \bmod d_i$ and $y_i \bmod L_i$, while keeping y_i still fixed mod Q_i, and thus gives another set $S(n, N)$.

For any divisor v of N, the leaders for the cycles whose position numbers have with N the g.c.d. v can be obtained by multiplying the elements of the set $S(n, N/v)$ by v. The work can be arranged so that all the sets $S(n, N/v)$ for all divisors v of N are constructed in one operation, without duplication of effort. This will be illustrated by an example. The example will also make use of the obvious fact that if N is double an odd, $S(n, N)$ can be derived from $S(n, N/2)$ by simply taking the latter elements and adding $N/2$ to those of them which are even.

4. Example. Let $m = 75$, $n = 73$. Then $N = mn - 1 = 5474 = 2 \cdot 7 \cdot 17 \cdot 23$; 73 is $3^1 \bmod 7$, $3^5 \bmod 17$, $5^4 \bmod 23$.

	p^t	$\phi(p^t)$	u	d	K	Q	L	y	e	Mg^{e+dy}
a)	7	6	1	1	6	3	2	0, 3	0	$391 \cdot 3^x$, $x = e + dy = 0$ or 3
b)	7	6	1	1	6	6	1	0	0	$391 \cdot 3^x$, $x = 0$
	17	16	5	1	16	16	1	0	0	$161 \cdot 3^x$, $x = 0$
	23	22	4	2	11	11	1	0	0, 1	$119 \cdot 5^x$, $x = 0$ or 1.

Notice that row a), with 2 not a factor of Q, is used when 17 is a factor of the modulus, since then the highest power of 2 occurs in $K(17)$. To get the four leaders of primitive cycles mod $7 \cdot 17 \cdot 23$, add either 391 or 2346 to either 119 or 595, and to 161. To get leaders for products by 17 of primitive cycles mod $7 \cdot 23$, add 391 (from row b)) to either 119 or 595—and so forth. The results, with the residues adjusted to be odd as explained earlier, are: 365, 671, 1147, 5363; 3017, 3493; 3247, 3723; 2507, 3289; 391; 161; 119, 595; 2737; also, their doubles, 730, $\cdots$, 1190, 0,—thirty leaders in all.

5. Comments. (i) This technique applies to the determination of leaders of cycles under multiplication by powers of n, in the ring of residues modulo N, if n and N are coprime,—regardless of the matrix interpretation.

(ii) For each prime-power p^t in N, a listing must be given for each power p^s ($s = 1, \cdots, t$), except that 2^1 can be omitted as indicated. In all these, the index u (or the two indices if $p = 2$) need not be changed for $g^u \equiv n \pmod{p^t}$ implies $g^u \equiv n \pmod{p^s}$. Each power p^s should have as many listings as there are different values Q possible for it.

(iii) It is interesting that certain partial sums of the terms in the classical expression (5) give (with appropriate modifications of the exponents) the imprimitive leaders.

Illinois Institute of Technology, Chicago, Illinois
Northwestern University, Evanston, Illinois